Knowmad Institut gemeinnützige UG (haftungsbeschränkt)
Germany | contact@knowmadinstitut.org | knowmadinstitut.org
DOI: 10.5281/zenodo.12668116

05.07.2024

Knowmad Institute's Final Report of Recommendations on the UN Cybercrime Convention (May 2024)

FINAL COMMENTS AND RECOMMENDATIONS TO THE AD HOC COMMITTEE TO ELABORATE A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES, ON THE UPDATED TEXT OF THE CONVENTION DATED MAY 2024.

European Institute for Multidisciplinary Studies on Human Rights and Sciences - Knowmad Institut.

Special Task Force:
Bp. Martin Ignacio Díaz Velásquez, Prof. Jorge Vicente Paladines, PhD. Leticia Fuentes Vera, Eng. Jesús Alfredo Ribero Faria, MSc. Oscar Hugo Espin García, Rev. Daniela Kreher, MSc. Ludwing Moncada Bellorin.

INTRODUCTION

The **Knowmad Institut - European Institute for Multidisciplinary Studies on Human Rights and Sciences**, committed to promoting human dignity and sustainable development, presents the following comments and recommendations for the updated text of the **International Convention On Countering The Use Of Information And Communications Technologies For Criminal Purposes (*A/AC.291/22/Rev.3*)**. These recommendations are based on a detailed analysis of the draft convention, the supplementary documents with references *A/AC.291/25/Rev.1* and *A/AC.291/27*, and the previous contributions of the Knowmad Institute to this distinguished committee (***Recs. 3ra Sesión***; ***Recs. 4ta Sesión***). Our approach focuses on ensuring that the convention protects human rights and dignity, promotes international cooperation, and adopts a balanced and effective approach to combating cybercrime.

Note: This document is a condensed version of our comprehensive analysis and comments, which are available here.

Knowmad Institut gemeinnützige UG (haftungsbeschränkt)
Germany | contact@knowmadinstitut.org | knowmadinstitut.org
DOI: 10.5281/zenodo.12668116

PREAMBLE

The Knowmad Institute, known for its multidisciplinary approach to human rights and science studies, has actively participated in previous sessions of the Ad Hoc Committee to elaborate a comprehensive international convention against the criminal use of information and communication technologies (ICT). In our previous contributions, we emphasized the importance of a balanced and comprehensive approach that respects the right to anonymity and personal data protection to create safe spaces in cyberspace. However, the most crucial aspect we highlighted was the need for promoting and protecting human rights to be the primary objectives when regulating ICT. This ensures that access to technology improves the quality of life without infringing on rights and freedoms, a principle of utmost importance.

We proposed the inclusion of a specific clause to protect vulnerable groups and prioritize the inclusive representation of individuals exposed to conflicts or persecutions of a political, ethnic, religious, or migratory nature. Furthermore, we emphasized the need to adopt an intersectional human rights approach with a gender perspective and the relevance of open science as a tool to prevent the criminal use of information and communication technologies (ICT). We consider it particularly urgent to address the potential threats of persecution due to migratory origin, recognizing that the diversity of dialects, especially in regions of the global south, can be mistakenly interpreted as an “encryption” method for possible criminal messages. This perspective is essential to strengthen international cooperation in preventing cybercrime and hybrid crimes, as well as in the interception of telecommunications, ensuring an inclusive and non-discriminatory approach to crime prevention.

We underscore the collective concern about the challenges posed by outsourced espionage services and intelligence gathering, highlighting the need for rigorous regulation and oversight to protect the physical integrity of individuals within organized civil society in particular and society in general. Additionally, we addressed the issue of trafficking controlled substances via the Internet and its impact on public health, suggesting harm reduction and deflection strategies to mitigate the adverse effects on the community.

Knowmad Institut gemeinnützige UG (haftungsbeschränkt)
Germany | contact@knowmadinstitut.org | knowmadinstitut.org
DOI: 10.5281/zenodo.12668116

RECOMMENDATIONS

Our recommendations and comments on the draft convention identified as ***A/AC.291/22/Rev.3*** emphasize the protection of human rights and privacy, aligning with international standards such as the International Covenant on Civil and Political Rights. The importance of updating and clarifying definitions regarding emerging technologies is highlighted to ensure effective and adaptive regulation.

Our recommendations and comments on the draft convention identified as A/AC.291/22/Rev.3 emphasize the protection of human rights and privacy, aligning with international standards such as the International Covenant on Civil and Political Rights. We highlight the importance of updating and clarifying definitions regarding emerging technologies to ensure effective and adaptive regulation.

We propose the incorporation of independent oversight and evaluation mechanisms that involve civil society, ensuring that the measures adopted are fair and respect human rights. Additionally, we recommend implementing educational and preventive programs to raise awareness about ICT security and mitigate the risks associated with cybercrime.

It is advised to clearly define the actions that constitute crimes in the digital realm and establish proportional sanctions that are both deterrent and commensurate with the severity of the offenses. Special protection for minors and the promotion of international cooperation to combat online child abuse are also suggested.

Fostering international cooperation and harmonizing laws is emphasized for a coordinated and effective response against cybercrime. This includes clarifying jurisdiction and improving legal procedures to facilitate efficient investigations and prosecutions.

The recommendations also address the importance of protecting personal data during international transfers and establishing clear regulations for extradition that respect human rights. Once personal data has been used, it should be deleted depending on the case. Additionally, it is recommended that the transfer of criminal proceedings be facilitated and mutual legal assistance between states be improved to strengthen the global fight against cybercrime.

Furthermore, the need to create and strengthen laws in the States Parties to protect witnesses and whistleblowers from retaliation, including intimidation and

DOI: 10.5281/zenodo.12668116

harassment, is underscored. This requires establishing witness protection programs, which include specific measures such as physical protection or relocation, as well as mechanisms for non-disclosure of information regarding the identity and whereabouts of witnesses.

In this regard, it is proposed to apply protection measures to both victims and witnesses, providing psychological and legal support so they can testify without fear of reprisals. It is also suggested that these witnesses and whistleblowers of cybercrimes be monitored to ensure the effectiveness of the protection measures.

Finally, we recommend adopting international standards, such as those of the Budapest Convention, to align standards and facilitate global cooperation. This includes consulting with experts and stakeholders to recommend robust reforms with clear definitions that ensure the proportionality of penalties, as well as strengthening the technological infrastructure to detect and effectively respond to cybercrime. Training judges, prosecutors, and law enforcement officers are essential to ensure the proper handling of crimes committed in cyberspace or in a hybrid manner within the judicial system. Public awareness campaigns can help prevent these crimes by informing citizens about risks and protection measures.

In summary, our recommendations aim to establish a robust framework that respects human rights and dignity, enabling the effective prevention and prosecution of cybercrime while protecting individuals' integrity and privacy in the digital environment. Implementing these measures will promote balanced and effective international cooperation while ensuring human dignity and sustainable development.

Note: This document is a condensed version of our comprehensive analysis and comments, which are available here.

Thematic Recommendations

Protection of Human Rights and Privacy

- **Incorporation in Articles:** Article 1, Article 6.
- **Detail:** Ensure that all measures adopted respect human rights and privacy by explicitly referencing existing human rights frameworks, such as the International Covenant on Civil and Political Rights (ICCPR) (United Nations,

DOI: 10.5281/zenodo.12668116

1966). This approach protects fundamental freedoms and reinforces the legitimacy of actions against cybercrime (Meier et al., 2020; Ali et al., 2022; Montal & Pauselli, 2023; Ajoy, 2022; Da-Yu Kao et al., 2019; Feldle, 2020; Kennedy & Warren, 2020; Ahsan et al., 2022).

Clear and Updated Definitions

- **Incorporation in Articles:** Article 2, Article 3.
- **Detail:** Include additional definitions reflecting emerging technologies such as Artificial Intelligence, the Internet of Things (IoT), and blockchain. Establish a mechanism for the periodic review and update of definitions to ensure their continuous relevance (Weber, 2009; Lobach et al., 2021; Aulia, 2023; Han, 2023; Klevtsov, 2020; Varshney et al., 2020; Balajanov, 2018).

Oversight and Evaluation Measures

- **Incorporation in Articles:** Article 6, Article 24.
- **Detail:** Establish independent oversight and evaluation mechanisms to ensure that measures adopted under the convention align with international human rights standards. The creation of oversight committees and the involvement of civil society organizations and other stakeholders are highly recommended (Cross, 2017; Curtis & Oxburgh, 2023; Holt, 2018; Mantovani, 2020; Nurahman, 2019; Brenner & Clarke, 2009).

Preventive and Educational Measures

- **Incorporation in Articles:** Article 7, Article 8, Article 9, Article 11.
- **Detail:** In addition to criminalization, include provisions on preventive measures and educational programs to raise societal awareness about ICT security and prevent cybercrime incidents (Krastev, 2022; ECPAT International, 2016; Gunarto et al., 2023; Grauer, 2022; Saxena, 2023; Cerezo et al., 2007; Kagita et al., 2020).

Clarification of Scope and Sanctions

- **Incorporation in Articles:** Article 10, Article 12, Article 13.
- **Detail:** Clearly define what constitutes interference and falsification in the context of electronic data and systems. Establish proportional and effective sanctions, adjusted to the severity of the offense, ensuring that the sanctions are both deterrent and just (Aldridge et al., 2017; Ajoy, 2022; Kaur, 2021; Sabu et al., 2023; Sprott, 2006; Khan et al., 2022).

DOI: 10.5281/zenodo.12668116

Protection of Minors and Special Measures

- **Incorporation in Articles:** Article 14, Article 15, Article 16.
- **Detail:** Clearly define "child sexual abuse material," "solicitation," and "harassment" to avoid ambiguous interpretations that may result in legal loopholes and ineffective protection for minors. Include coordinated support and rehabilitation mechanisms for victims, and promote international cooperation to prevent and prosecute online child sexual abuse (Interpol, 2022; Bunga & Hiariej, 2019; Henry et al., 2020; Irawan et al., 2022; Citron & Franks, 2014; Knowmad Institute, 2023).

International Cooperation and Harmonization of Laws

- **Incorporation in Articles:** Article 17, Article 18, Article 19, Article 22, Article 23.
- **Detail:** Foster international cooperation and harmonization of laws among Member States to ensure a coordinated and effective response to cybercrime. Establish clear coordination and collaboration mechanisms (Broadhurst, 2017; Skulysh, 2014; Wingfield & Wingo, 2021; Dragomir, 2022; McGlynn & Rackley, 2017; Mabeka & Cassim, 2023).

Jurisdiction and Law Enforcement

- **Incorporation in Articles:** Article 19, Article 21, Article 24, Article 25.
- **Detail:** Ensure that Member States clearly define the limits and scope of their jurisdiction over cybercrimes and adopt legislative measures that allow for the effective implementation of the necessary powers and procedures for investigations and prosecutions (Hursevich, 2019; PTACC, 2022; Nurahman, 2020; Ruslan, 2023; Wilson, 2008; Setiawahyudi, 2015; Snail, 2009; Szongoth & Vetter, 2018; Teichmann & Wittmann, 2022; Tiutiuhin, 2022; Veresha, 2018; Voynova, 2015; Wicki-Birchler, 2020).

Preservation and Partial Disclosure of Traffic Data

- **Incorporation in Articles:** Article 26.
- **Detail:** Ensure the prompt preservation of traffic data, even when multiple service providers are involved. Implement clear procedures for the rapid disclosure of traffic data to competent authorities. The convention could specify the timeframes and conditions under which service providers must provide this data (Wicki-Birchler, 2020; Saxena, 2023).

Knowmad Institut gemeinnützige UG (haftungsbeschränkt)
Germany | contact@knowmadinstitut.org | knowmadinstitut.org
DOI: 10.5281/zenodo.12668116

Production Order

- **Incorporation in Articles:** Article 27.
- **Detail:** Adopt clear legislative measures specifying the procedures and requirements for issuing production orders. Include adequate safeguards to protect individuals' privacy and rights when production orders are issued. Promote transparent collaboration between competent authorities and service providers for user data (Curtis & Oxburgh, 2023; Wicki-Birchler, 2020; Saxena, 2023).

Search and Seizure of Stored Electronic Data
Real-Time Collection of Data

- **Incorporation in Articles:** Article 28, Article 29.
- **Detail:** Specify the procedures for the search and seizure of electronic data and the real-time collection of data, ensuring that competent authorities can act efficiently and within the established legal framework. Include provisions to maintain the integrity and security of electronic data during and after its collection or seizure. Promote collaboration with experts in information technology, telecommunications, and ethics (Curtis & Oxburgh, 2023; Feldle, 2020; Da-Yu Kao et al., 2019; Wicki-Birchler, 2020; Saxena, 2023).

Content Data Interception

- **Incorporation in Articles:** Article 30.
- **Detail:** Specify the procedures and requirements for intercepting content data, ensuring that competent authorities can act efficiently and within the established legal framework. Mandate service providers to fully cooperate with competent authorities and maintain the technical capability to intercept and record content data in real time. Include provisions to ensure the confidentiality of content data interception (Clough, 2015; Han, 2023; Sabu et al., 2023).

Freezing, Seizing, and Confiscating Crime Proceeds

- **Incorporation in Articles:** Article 31.
- **Detail:** Implement clear legislative measures to allow the confiscation of proceeds of crime and assets used in the commission of cybercrimes. Ensure that authorities have the legal and technical tools necessary to identify, trace, and freeze assets related to cybercrimes. Establish clear procedures for the administration of frozen, seized, or confiscated assets (Setiawahyudi, 2015; Snail, 2009; Rajaan & Dadhich, 2020).

DOI: 10.5281/zenodo.12668116

Establishment of a Criminal Registry

- **Incorporation in Articles:** Article 32.
- **Detail:** Adopt legislative measures that allow the consideration of prior convictions from other States in national criminal proceedings. Establish international cooperation mechanisms to facilitate the exchange of information on prior convictions between States. Include safeguards to protect the rights of the accused (Tiutiuhin, 2022; Sprott, 2006; Papai-Tarr, 2020).

Witness Protection

- **Incorporation in Articles:** Article 33.
- **Detail:** Create and strengthen laws to protect witnesses and whistleblowers from retaliation, including intimidation and harassment. Establish specific measures such as physical protection or relocation and create mechanisms for the non-disclosure of information about the identity and whereabouts of witnesses. Apply protection measures to both victims and witnesses, providing psychological and legal support (Sarkar & Shukla, 2023; Nurahman, 2020).

Assistance and Protection for Victims

- **Incorporation in Articles:** Article 34.
- **Detail:** Implement legislative measures to guarantee assistance and protection for victims of cybercrimes, including mechanisms for psychological and physical support. Establish clear procedures for victims to obtain compensation and restitution. Include the opinions and concerns of victims in criminal proceedings (Mabeka & Cassim, 2023; Agung et al., 2023; Veresha, 2018).

General Principles of International Cooperation

- **Incorporation in Articles:** Article 35.
- **Detail:** Strengthen international cooperation mechanisms, ensuring clear and effective protocols for collaboration in cybercrime investigations. Harmonize national legislation with international standards (Klevtsov, 2020; Cerezo et al., 2007; Skulysh, 2014).

Protection of Personal Data

- **Incorporation in Articles:** Article 36.
- **Detail:** Adopt clear legislative measures regulating the transfer of personal data in accordance with national and international laws. Establish bilateral or multilateral agreements to facilitate the secure transfer of personal data.

DOI: 10.5281/zenodo.12668116

Ensure that received personal data is subject to effective and appropriate safeguards (Gulczyńska, 2021; Mantovani, 2020; Buković, 2020).

Transfer of Criminal Proceedings

- **Incorporation in Articles:** Article 39.
- **Detail:** Adopt legislative measures that facilitate the transfer of criminal proceedings. Establish bilateral or multilateral agreements to facilitate the transfer of criminal proceedings that respect the human rights of the accused (Voynova, 2015; Klevtsov, 2020; Hursevich, 2019).

General Principles and Procedures Related to Mutual Legal Assistance

- **Incorporation in Articles:** Article 40.
- **Detail:** Adopt clear legislative measures and procedures to facilitate mutual legal assistance in cybercrime investigations. Promote international collaboration through bilateral and multilateral agreements. Ensure that mutual legal assistance procedures respect the human rights of all parties involved (Hunton, 2012; Wilson, 2008; Mabeka & Cassim, 2023).

FINAL CONSIDERATIONS

The Knowmad Institute urges the Ad Hoc Committee to consider these recommendations to ensure that the proposed convention not only effectively combats cybercrime but also respects and protects human rights and fundamental freedoms. Implementing these recommendations will promote balanced and effective international cooperation while guaranteeing human dignity and sustainable development.

Additionally, the convention must consider and mitigate any potential misuse of surveillance technologies. We are concerned that the convention's approach could be interpreted and used to justify mass surveillance that infringes on fundamental rights to privacy and free movement, especially in the Global North, and that this would disproportionately affect migrant and displaced populations. Clear and strict safeguards must be established to prevent the instrumentalization of these measures against vulnerable groups, ensuring that any actions taken under this convention are carried out with full respect for human rights and fundamental freedoms in accordance with the principles established in the United Nations Charter.

DOI: 10.5281/zenodo.12668116

Cybercrime is a phenomenon that can affect daily activities, compromise privacy, and violate the rights of those who use technologies and the internet. Given its range (from economic fraud to cyberbullying and the most severe offenses related to child sexual exploitation and others that deeply endanger and violate people's rights and dignity), it is essential that the Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes explicitly references international human rights frameworks, such as the International Covenant on Civil and Political Rights (ICCPR) of the United Nations. This will ensure that measures against cybercrime align with international human rights standards, reinforce their legitimacy, and foster cooperation among Member States.

Secondly, continuous updating of definitions and measures against cybercrime is necessary, as the dynamics of coexistence, socialization, transaction, and even decision-making and development of activities in the social, political, and cultural spheres in cyberspace are renewed and transformed rapidly. This has created gaps and inequalities in terms of access to and delivery of justice when fundamental rights are violated. This also implies clarifying key terms, starting with cybercrime and its modalities, to avoid ambiguous use that could lead to misleading interpretations. It is proposed that examples be used when technical terms are employed.

It is essential to clarify the scope of the definition of offenses, specifying that these can be committed by natural persons, legal entities, and state and parastatal entities. It includes espionage perpetrated by these entities against activists, journalists, and other civil society actors.

It is crucial to implement educational and awareness programs on ICT security and cybercrime prevention. These programs should be designed to inform users about the risks associated with ICT use and include recommendations and preventive measures in the various spheres of users' development. It is also essential to have procedures to recover and preserve information, as necessary, to minimize the impact of any incident in cyberspace or hybrid space.

In this regard, another critical aspect is comprehensive support for victims of cybercrimes, including counseling and legal assistance services. For this to be effective, prevention programs should be backed by continuous human rights training for law enforcement officers, judges, prosecutors, and victim support staff, such as doctors, psychologists, and social workers, on the rights and needs of victims to foster a culture of empathy and support, aiming to promote a culture of respect and protection in all related actions and decisions.

Knowmad Institut gemeinnützige UG (haftungsbeschränkt)
Germany | contact@knowmadinstitut.org | knowmadinstitut.org
DOI: 10.5281/zenodo.12668116

The International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights enshrined the right to access justice. Therefore, Member States must ensure that individuals (regardless of nationality, ethnic origin, migratory background, gender, creed, or ideology) can access and defend their rights in fair and impartial processes. This relates to the sanctions resulting from these processes, which must be proportional and effective, as not all cybercrimes have the same impact. Therefore, sanctions can range from complementary measures linked to cybersecurity education programs, deterrent economic penalties for restitution to cybercrime victims, and even imprisonment.

We call on Member States to maintain a human rights-centered approach when formulating and applying measures against cybercrime, protecting and promoting the dignity of every individual. Only then can we build a safe and just digital environment for all.

European Institute for Multidisciplinary Studies on Human Rights and Sciences - Knowmad Institut.

Grupo Especial de Trabajo:

Ob. Martin Ignacio Díaz Velásquez, Prof. Jorge Vicente Paladines, Dra. Leticia Fuentes Vera, Ing. Jesús Alfredo Ribero Faria, MSc. Oscar Hugo Espin García, Rev. Daniela Kreher, MSc. Ludwing Moncada Bellorin.

Note: This document is a condensed version of our comprehensive analysis and comments, which are available here.

REFERENCES

1. Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., & Rifat, N. (2022). Cybersecurity threats and their mitigation approaches using machine learning—A review. *Journal of Cybersecurity and Privacy, 2*(3), 527-555. https://doi.org/10.3390/jcp2030027
2. Ali, A., Khan, I., & Bashir, S. (2022). Need of international legislation regarding cyber crimes: Pakistan perspective. *Pakistan Journal of Social Research, 4*(2), 45-55. https://doi.org/10.52567/pjsr.v4i2.608
3. Aldridge, J., Stevens, A., & Barratt, M. J. (2017). Will growth in cryptomarket drug buying increase the harms of illicit drugs? *Addiction, 113*(5), 789-796. https://doi.org/10.1111/add.13899

DOI: 10.5281/zenodo.12668116

4. Ajoy, P. B. (2022). Effectiveness of criminal law in tackling cybercrime: A critical analysis. *Scholars International Journal of Law, Crime and Justice, 5*(2), 75-85. https://doi.org/10.36348/sijlcj.2022.v05i02.005
5. Aulia, A. (2023). Adoption of the law on information and electronic transactions against cyber crime. *Scholars International Journal of Law, Crime and Justice, 6*(3), 1-7. https://doi.org/10.36348/sijlcj.2023.v06i03.001
6. Balajanov, E. (2018). Setting the minimum age of criminal responsibility for cybercrime. *International Review of Law, Computers & Technology, 32*(1), 102-115. https://doi.org/10.1080/13600869.2018.1417764
7. Brenner, S. W., & Clarke, L. L. (2009). Combatting cybercrime through distributed security. *International Journal of Intercultural Information Management, 1*(3), 259. https://core.ac.uk/download/pdf/76622895.pdf
8. Broadhurst, R. (2017). Cybercrime: Thieves, swindlers, bandits and privateers in cyberspace. *SSRN*. https://doi.org/10.2139/ssrn.3009574
9. Bunga, D. (2019). Legal response to cybercrime in global and national dimensions. *Padjadjaran Journal of International Law, 6*(1), 45-57. https://doi.org/10.22304/pjih.v6n1.a4
10. Bunga, D., & Hiariej, O. S. (2019). Cyberbullying on children in victimology perspective. *Scholars International Journal of Law, Crime and Justice, 2*(2), 116-121. https://doaj.org/article/74dfa3150c9d4afdabdb5a24672dae82
11. Caneppele, S., & Aebi, M. F. (2017). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice, 13*(1), 66-79. https://doi.org/10.1093/police/pax055
12. Cerezo, A., Lopez, J., & Patel, A. (2007). International cooperation to fight transnational cybercrime. *Proceedings of the 21st International Conference on Advanced Communication Technology (ICACT)*. https://doi.org/10.1109/WDFIA.2007.7
13. Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. *Wake Forest Law Review, 49*, 345+. U of Maryland Legal Studies Research Paper No. 2014-1. https://ssrn.com/abstract=2368946
14. Clough, J. (2015). Principles of cybercrime: Interception of data. *Cambridge University Press*. https://doi.org/10.1017/CBO9781139540803.007
15. Cross, D. (2017). A human rights-based approach to community justice: Adding value to desistance focused practice. *European Journal of Probation, 9*(2), 67-84. https://doi.org/10.1177/2066220317719801
16. Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal, 96*(4), 573-592. https://doi.org/10.1177/0032258X221107584
17. Da-Yu Kao, E., Chang, E.-C., & Tsai, F. (2019). Extracting suspicious IP addresses from WhatsApp network traffic in cybercrime investigations. *Proceedings of the 21st International Conference on Advanced Communication Technology (ICACT)*. https://doi.org/10.23919/ICACT.2019.8701941

DOI: 10.5281/zenodo.12668116

18. Dragomir, B. (2022). Mechanisms of international cooperation against cybercrime. *Proceedings of the International Conference on Cybercrime, 70*(1), 55-68. https://doi.org/10.36997/ppdd2022.70
19. ECPAT International. (2016). Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales. *ECPAT Luxembourg*. https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines_Spanish_version-electronica_FINAL.pdf
20. Feldle, J. (2020). Zivilrechtliche Haftung im automatisierten Straßenverkehr – Hackerangriffe, Sicherheitserwartungen und erlaubte Nebentätigkeiten. *Nomos*. https://doi.org/10.5771/9783748920984-199
21. Geldenhuys, K. (2021). Spyware. *Servamus Community-Based Safety and Security Magazine, 114*(10), 15-17. https://doi.org/10.10520/ejc-servamus_v114_n10_a5
22. Grauer, K. (2022). The 2022 crypto crime report. *Chainalysis*. https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf
23. Gunarto, G., Jainah, J., & Mashdurohatun, A. (2023). Legal reconstruction of trafficking victim protection based on justice value. *Scholars International Journal of Law, Crime and Justice, 6*(5), 25-32. https://doi.org/10.36348/sijlcj.2023.v06i05.005
24. Han, Y. (2023). Research and application of pseudo-information detection technology based on computer information hiding. *Proceedings of the 21st International Conference on Advanced Communication Technology (ICACT)*. https://doi.org/10.1109/ACCTCS58815.2023.00067
25. Henry, N., Flynn, A., & Powell, A. (2020). Technology-facilitated domestic and sexual violence: A review. *Violence Against Women, 26*(7), 761-788. https://doi.org/10.1177/1077801219841445
26. Holt, T. (2018). Regulating cybercrime through law enforcement and industry mechanisms. *Annals of the American Academy of Political and Social Science, 678*(1), 140-157. https://doi.org/10.1177/0002716218783679
27. Hursevich, A. (2019). Ube international legal cooperation of the prosecutor general's office of the republic of belarus in the fight against cybercrime and typical examples of committing such crimes. *RAESMPCE, 11*(2). https://doi.org/10.54275/raesmpce.v11i2.96
28. Irawan, J., Nathaniel, A., & Jonathan, S. (2022). Juridical analysis about cyberbullying cases by child perpetrators against child victims. *De Jure: Jurnal Hukum Dan Siyasah, 22*(1), 17-32. https://doi.org/10.30641/dejure.2022.v22.17-32
29. Interpol. (2022). Terminología apropiada. Recuperado de https://www.interpol.int/es/Delitos/Delitos-contra-menores/Terminologia-apropiada
30. Kagita, M. K., Thilakarathne, N., Gadekallu, T. R., Maddikunta, P. K. R., & Singh, S. (2020). A review on cyber crimes on the internet of things. *ArXiv*. https://arxiv.org/abs/2009.05708
31. Kaur, S. (2021). Security in cyber crime. *International Journal of Recent Advances in Science and Technology, 9*(5), 123-135. https://doi.org/10.22214/ijraset.2021.38023

DOI: 10.5281/zenodo.12668116

32. Kennedy, S., & Warren, I. (2020). The legal geographies of extradition and sovereign power. *Internet Policy Review, 9*(3), 1-22. https://doi.org/10.14763/2020.3.1496
33. Khan, S., Saleh, T., Dorasamy, M., Tan Swee Leng, O., & Gale Vergara, R. (2022). A systematic literature review on cybercrime legislation. *F1000Research, 11*, 971. https://doi.org/10.12688/f1000research.123098.1
34. Klevtsov, K. (2020). International cooperation in the fight against cybercrime: Current state and development prospects. *SSRN*. https://doi.org/10.2139/ssrn.3728311
35. Knowmad Institut. (2023). TERCERA SESIÓN: COOPERACIÓN INTERNACIONAL, ASISTENCIA TÉCNICA, MEDIDAS DE PREVENCIÓN Y MECANISMO DE APLICACIÓN. Recuperado de https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Documents/Knowmad-_ES_3rd_Session.pdf
36. Krastev, D. B. (2022). Mechanisms of international cooperation against cybercrime. *International Journal of Cybersecurity, 70*(2), 155-167. https://doi.org/10.36997/ppdd2022.70
37. Lobach, D. V., Shestopal, S. S., & Smirnova, N. L. (2021). The phenomenon of cyber crime in the focus of conceptual legal analysis. *European Proceedings of Social and Behavioural Sciences, 6*(3), 385-392. https://doi.org/10.15405/epsbs.2021.06.03.77
38. Mabeka, N. Q., & Cassim, F. (2023). Interpreting the provisions of the Cybercrimes Act 19 of 2020 in the context of civil procedure: A future journey. *Obiter, 44*(1). https://doi.org/10.17159/obiter.v44i1.15886
39. Mantovani, M. (2020). Contractual obligations as a tool for international transfers of personal data under the GDPR. *SSRN*. https://doi.org/10.2139/ssrn.3522426
40. McGlynn, C., & Rackley, E. (2017). Image-based sexual abuse. *Oxford Journal of Legal Studies, 37*(3), 534-561. https://doi.org/10.1093/ojls/gqw033
41. Meier, B. M., Huffstetler, H. E., & de Mesquita, J. B. (2020). Monitoring and review to assess human rights implementation. *International Journal of Human Rights, 24*(3), 256-270. https://doi.org/10.1093/oso/9780197528297.003.0008
42. Montal, F., & Pauselli, G. (2023). Is the bad news about compliance bad news about human rights? Evidence from the Inter-American Commission on Human Rights. *International Studies Quarterly, 67*(1), 85-97. https://doi.org/10.1093/isq/sqad027
43. Naciones Unidas. (1966). Pacto Internacional de Derechos Civiles y Políticos. Recuperado de https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
44. Naciones Unidas. (1966). Pacto Internacional de Derechos Civiles y Políticos. Recuperado de https://www.ohchr.org/sites/default/files/ccpr_sp.pdf
45. Naciones Unidas. (2016). Promoción, protección y disfrute de los derechos humanos en Internet. *A/HRC/32/L.20*. Recuperado de https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_32_L20.pdf
46. Nurahman, D. (2019). Kebijakan penegakan hukum cybercrime dan pembuktian yuridis dalam sistem hukum pidana nasional. *Jurnal Keadilan, 17*(2), 270-284. https://doi.org/10.37090/keadilan.v17i2.270

DOI: 10.5281/zenodo.12668116

47. Nurahman, D. (2020). Cybercrime Policies: Juridical Evidence and Law Enforcement Policies. *CCER*, 101. http://dx.doi.org/10.4108/eai.26-9-2020.2302579
48. PTACC | Police Treatment and Community Collaborative. (2022). Best practices in law enforcement and community responses. Recuperado de https://ptaccollaborative.org/
49. Ruslan, A. R. (2023). International legal regulation of the fight against cybercrime. *Journal of International Law, 24*(3), 24-30. https://doi.org/10.37399/issn2072-909x.2023.4.24-30
50. Sabu, J., Ananthanarayanan, S., Gopan, A., G. S., & Murali, S. (2023). Advanced keylogger with keystroke dynamics. *Proceedings of the International Conference on Information and Communication Technology*. https://doi.org/10.1109/ICICT57646.2023.10134044
51. Sarkar, G., & Shukla, S. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, *2*, 1-26. https://doi.org/10.1016/j.jeconc.2023.100034
52. Saxena, M. (2023). Impact of cybercrime on e-governance. Is cybercrime affecting the confidentiality of government data? *International Journal of Cyber Criminology*. https://doi.org/10.21275/sr231111140516
53. Setiawahyudi, A. (2015). Kendala pertanggungjawaban pidana terhadap pelaku pencurian uang di bank melalui internet berdasarkan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. *Majalah Hukum, 21*(2), 145-167. https://dx.doi.org/10.30996/mk.v0i0.2116
54. Skulysh, I. (2014). International legal cooperation in the field of combating cybercrime. *Journal of Law and Political Sciences, 10*(1), 272-432. https://doi.org/10.37750/2616-6798.2014.1(10).272432
55. Snail, S. (2009). Cyber crime in South Africa - Hacking, cracking, and other unlawful online activities. *Journal of Information Law & Technology, 10*(2), 127-145. https://dblp.org/rec/journals/jilt/Snail09.html
56. Sprott, J. B. (2006). The use of custody for failing to comply with a disposition cases under the Young Offenders Act. *Canadian Journal of Criminology and Criminal Justice, 48*(3), 251-271. https://doi.org/10.1353/ccj.2006.0043
57. Szongoth, R., & Vetter, D. (2018). Nemzetközi bűnügyi együttműködés a kiberbűnözés területén. *Budapesti Szemle, 7-8*(1), 45-60. https://doi.org/10.38146/bsz.2018.7-8.1
58. Teichmann, F., & Wittmann, C. (2022). When is a law firm liable for a data breach? An exploration into the legal liability of ransomware and cybersecurity. *Journal of Financial Crime, 29*(3), 819-832. https://doi.org/10.1108/jfc-04-2022-0093
59. Tiutiuhin, V. I. (2022). Conviction as one of the means of criminal responsibility. *Journal of Law and Political Sciences, 18*(1), 267-249. https://doi.org/10.21564/2311-9640.2022.18.267249
60. UNODC. (2021). World drug report 2021. *United Nations: Office on Drugs and Crime*. https://www.unodc.org/unodc/en/data-and-analysis/wdr2021.html

DOI: 10.5281/zenodo.12668116

61. Varshney, S., Munjal, D., Jash, I., Bhattacharya, O., & Saboo, S. (2020). Cyber crime awareness and corresponding countermeasures. *SSRN*. https://doi.org/10.2139/ssrn.3601807
62. Veresha, R. (2018). Preventive measures against computer related crimes. *Interdisciplinary Management Research, 14*, 227-243. https://doi.org/10.32914/I.51.3-4.7
63. Voynova, R. (2015). Comparison of the transfer of criminal proceeding with other forms of international legal cooperation in criminal matters. *Sciendo*. https://doi.org/10.1515/kbo-2015-0091
64. Weber, R. (2009). Internet of things–Need for a new legal environment? *Computer Law & Security Review, 25*(6), 522-527. https://doi.org/10.1016/j.clsr.2009.09.002
65. Wicki-Birchler, D. (2020). The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?. *Int. Cybersecur. Law Rev.* 1, 63–72. https://doi.org/10.1365/s43439-020-00012-5
66. Wilson, N. (2008). Forensics in cyber-space: The legal challenges. *International Journal of Digital Crime and Forensics, 3*(1), 56-70. https://doi.org/10.4108/E-FORENSICS.2008.2926
67. Wingfield, T., & Wingo, H. (2021). International law for cyberspace. *Oxford Handbook of Cybersecurity*. https://doi.org/10.1093/oxfordhb/9780198800682.013.37